

ORIGINAL

Approved: Kristy J. Greenberg
KRISTY J. GREENBERG
Assistant United States Attorney

Before: HONORABLE GABRIEL W. GORENSTEIN
United States Magistrate Judge
Southern District of New York

18 MAG . 5026

- - - - - X
: SEALED COMPLAINT
UNITED STATES OF AMERICA :
:
- v. - : Violations of
: 18 U.S.C. §§ 1343, 1956(h) &
: 2
:
WILLIAM McFARLAND, : COUNTY OF OFFENSE:
: NEW YORK
Defendant. :
:
- - - - - X

SOUTHERN DISTRICT OF NEW YORK, ss.:

BRANDON RACZ, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation (the "FBI"), and charges as follows:

Count One
(Wire Fraud)

1. From at least in or about late 2017, up to and including at least in or about March 2018, in the Southern District of New York and elsewhere, WILLIAM McFARLAND, the defendant, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations and promises, transmitted and caused to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, to wit, McFARLAND engaged in a sham ticket-selling business for exclusive events through a company controlled and operated by McFARLAND ("NYC VIP Access") by, among other things, making false representations that NYC VIP Access had tickets for sale to special events in fashion, music and sports, and in connection therewith and in furtherance thereof, McFARLAND caused

wire communications and wire transfers of funds to be sent in interstate commerce.

(Title 18, United States Code, Sections 1343 & 2.)

Count Two
(Money Laundering)

2. From at least in or about late 2017, up to and including at least in or about March 2018, in the Southern District of New York and elsewhere, WILLIAM McFARLAND, the defendant, in an offense involving and affecting interstate and foreign commerce, knowing that the property involved in certain financial transactions, to wit, wire transfers, represented the proceeds of some form of unlawful activity, willfully and knowingly would and did conduct and attempt to conduct such financial transactions which in fact involved the proceeds of specified unlawful activity, to wit, proceeds of the offense charged in Count One of this Complaint, knowing that the transactions were designed in whole and in part to conceal and disguise the nature, the location, the source, the ownership and the control of the proceeds of specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B).

(Title 18, United States Code, Section 1956(h).)

The bases for my knowledge and for the foregoing charge are, in part and among other things, as follows:

3. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). I have been an FBI Special Agent for approximately three years and I am assigned to a White Collar Fraud squad within the New York Division. As part of my work at the FBI, I have received training regarding fraud and white collar crimes. I am familiar with the facts and circumstances set forth below from my personal participation in the investigation, including my examination of reports and records, interviews I have conducted, and conversations with other law enforcement officers and other individuals. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements and conversations of others are reported herein, they are reported in substance and in part, unless noted otherwise.

THE DEFENDANT AND HIS COMPANIES

4. At all relevant times, WILLIAM McFARLAND, the defendant, owned and operated a company, based in New York, New York, which purported to be in the business of obtaining and selling for profit, tickets to various exclusive events including fashion galas, music festivals, and sporting events ("NYC VIP Access"). As discussed below, McFARLAND took steps to make the company appear as if it was controlled and operated by other individuals.

5. From in or about 2014, up to and including in or about 2017, WILLIAM McFARLAND, the defendant, was the founder and Chief Executive Officer of Magnises, a credit card and private club for millennials that sold tickets to exclusive events.

6. From in or about 2016, up to and including in or about 2017, WILLIAM McFARLAND, the defendant, was the founder and Chief Executive Officer of Fyre Media LLC ("Fyre Media"). In 2016, McFARLAND started Fyre Media to build a digital app that would allow individuals organizing commercial events, such as concerts, to bid for artist and celebrity bookings at such events.

7. In late 2016, WILLIAM McFARLAND, the defendant, established a subsidiary of Fyre Media known as Fyre Festival LLC and began promoting a music festival set to take place over two weekends in April 2016 in the Bahamas (the "Fyre Festival"). McFARLAND promoted the Fyre Festival in part by claiming that it would bring a global audience together to share a life changing experience. Ultimately, the Fyre Festival was widely deemed to have been a failure.

8. On March 6, 2018, WILLIAM McFARLAND, the defendant, pled guilty to before the Honorable Naomi Reice Buchwald, United States District Judge, to: (1) wire fraud in violation of Title 18, United States Code, Section 1343, in connection with a scheme to defraud over 80 investors in Fyre Media and Fyre Festival LLC of over \$24 million in losses; and (2) wire fraud in violation of Title 18, United States Code Section 1343, in connection with a scheme to defraud a ticket vendor for the Fyre Festival of \$2 million in losses. United States v. William McFarland, 17 Cr. 600 (NRB). McFARLAND has been on pretrial release since July 1, 2017, and is currently awaiting sentencing in that case.

OVERVIEW OF THE SCHEME TO DEFRAUD AND LAUNDER MONEY

9. As set forth below, WILLIAM McFARLAND, the defendant, while on pretrial release, perpetrated a scheme to defraud attendees of the Fyre Festival and others by soliciting them to purchase tickets from NYC VIP Access to exclusive events when, in fact, no such tickets existed. In soliciting ticket sales, McFARLAND used an email account in the name of a then-employee ("Employee-1") in order to hide his affiliation with NYC VIP Access. McFARLAND provided prospective customers with contracts that falsely represented that NYC VIP Access had tickets to exclusive events in fashion, music and sports. In order to distance himself from the operation, McFARLAND directed that Employee-1 sign the contracts between NYC VIP Access and the customers. After McFARLAND induced customers to wire money for tickets, McFARLAND either did not provide tickets at all, or did not provide tickets as advertised. In an effort to conceal his ownership and control of the ticket sale proceeds, McFARLAND instructed and caused ticket sale proceeds to be sent to a bank account belonging to Employee-1, or a mobile payment service account belonging to another employee ("Employee-2").

McFARLAND'S MISREPRESENTATIONS TO VICTIM-CUSTOMERS

10. Based on my discussions with a former employee of NYC VIP Access ("Employee-1") and another law enforcement agent who interviewed Employee-1, as well as reviewing that agent's notes and documents provided by Employee-1, I have learned, in substance and in part, the following:

a. In or about fall 2017, WILLIAM McFARLAND, the defendant, told Employee-1 that his new company, NYC VIP Access, was going to be similar to his former company Magnises, which McFARLAND stated had shut down only due to the bad press surrounding the Fyre Festival that tarnished his reputation. McFARLAND said that he still had access to tickets for exclusive high-end events through event sponsors, and offered Employee-1 a job in ticket sales for NYC VIP Access. McFARLAND offered to pay Employee-1 a salary of approximately \$300/week and 10% commission for any ticket sales that Employee-1 made on behalf of NYC VIP Access. Employee-1 agreed to work for McFARLAND at NYC VIP Access.

b. McFARLAND provided Employee-1 with a list of potential customers and their phone numbers, as well as a script; McFARLAND instructed Employee-1 to cold call prospective

customers and follow McFARLAND's script in order to sell tickets to events.

c. McFARLAND corresponded with customers from an email account in Employee-1's name at NYC VIP Access (the "Employee-1 Email Account"). McFARLAND told Employee-1 that McFARLAND emailed former Magnises customers about ticket sales to NYC VIP Access events. Employee-1 did not send any emails to customers from the Employee-1 Email Account.

d. NYC VIP Access purported to sell tickets to the following events, among others: the 2018 Met Gala, Burning Man 2018, Coachella 2018, the 2018 Grammy Awards, Super Bowl LII, and a Cleveland Cavaliers game and team dinner with Lebron James. During Employee-1's employment at NYC VIP Access, Employee-1 believed that McFARLAND had tickets to sell to these events. Employee-1 is not aware of any tickets that were actually provided to customers other than two customers ("Victim-4" and "Victim-8") who attended the Grammy Awards, but did not receive the premium tickets they were promised.

e. McFARLAND set up an account with a payment processor ("Payment Processor-1"), and arranged for customer payments made by wire transfer or Payment Processor-1 to be deposited into Employee-1's bank account (the "Employee-1 Bank Account").

11. Based on my discussions with another law enforcement agent who interviewed Employee-2, as well as reviewing that agent's notes and documents provided by Employee-2, I have learned, in substance and in part, the following:

a. In or about fall 2017, Employee-1 introduced Employee-2 to WILLIAM McFARLAND, the defendant, and Employee-2 became McFARLAND's assistant. NYC VIP Access was McFARLAND's company; all NYC VIP Access employees took orders from McFARLAND. McFARLAND was responsible for procuring tickets.

b. McFARLAND asked Employee-2 to use the contact information of Fyre Festival attendees to create a spreadsheet of prospective customers for NYC VIP Access. Employee-2 identified the Fyre Festival attendees with the highest salaries as prospective NYC VIP Access customers. At McFARLAND's direction, Employee-1 would cold call prospective customers to solicit them to purchase tickets for events.

c. McFARLAND sent emails to customers from the Employee-1 Email Account. McFARLAND regularly read or showed the emails he was drafting to customers from the Employee-1 Email Account to Employee-1 and Employee-2 before he sent them. At McFARLAND's direction, Employee-2 sent executed contracts to customers from the Employee-1 Email Account, but did not email with customers for any other purpose. Employee-1 did not send any emails to customers.

d. During Employee-2's employment at NYC VIP Access, Employee-2 believed that McFARLAND had tickets to sell to the events he advertised. Employee-2 is not aware of any tickets that were actually provided to customers other than two customers who attended the Grammy Awards.

e. McFARLAND received customers' credit card information from the Employee-1 Email Account and processed credit card payments. McFARLAND also used an account with another payment processor ("Payment Processor-2") in Employee-2's name (the "Employee-2 Payment Processor-2 Account") to accept customer payments.

12. Based on my review of payments from customer-victims to the Employee-1 Bank Account through Payment Processor-1 and wire transfers, and the Employee-2 Payment Processor-2 Account, as well as interviews conducted by myself and/or another law enforcement agent with Employee-1, Employee-2 and approximately 15 victims, and review of their documents, I believe that in total, WILLIAM McFARLAND, the defendant, charged at least approximately \$100,000 in fraudulent tickets to at least approximately 15 customer-victims. Three examples of McFARLAND's fraudulent ticket sales scam are described in more detail below.

The 2018 Met Gala Ticket Scam

13. Based on my discussions with Employee-1 and another law enforcement agent who interviewed Employee-1 and Employee-2, as well as reviewing that's agent's notes and emails sent from the Employee-1 Email Account, I have learned, in substance and in part, the following:

a. On or about December 17, 2017, WILLIAM McFARLAND, the defendant, sent email solicitations from the Employee-1 Email Account to a mass email list of prospective customers regarding ticket sales to the 2018 Met Gala held on April 30, 2018. The email with the subject "2018 MET GALA - Red Carpet & Gala Tickets" read as follows:

You asked, and we are now excited to announce that we are offering tickets to the 2018 Met Gala - the biggest single night of celebrity, fashion, and entertainment. The 2018 Met Gala is on Monday, April 30 at The Met in NYC. We partnered with the sponsoring brands to get you a chance to buy tickets. Tickets include red carpet, seats for the event/dinner, and an invitation to the after-party. Tickets are extremely limited. Please respond with your brief bio and number of guests you'd like to have attend, and we'll follow up with a call.

The email ends with the first name of Employee-1 and Employee-1's phone number.

b. McFARLAND told Employee-1 that they would sell tickets to the dinner and red carpet access for \$2,500 per ticket. McFARLAND stated that customers needed to submit a biography, and McFARLAND would decide who to accept for tickets.

c. According to Employee-1, one customer ("Victim-1") wanted email confirmation of Victim-1's ticket purchase from the Met Gala. When Employee-1 told McFARLAND, McFARLAND indicated that the customer would get the confirmation. McFARLAND then told Employee-1 that there was an email from the host of the 2018 Met Gala (the "Gala Host") to the Employee-1 Email Account in which the Gala Host confirmed Victim-1's tickets to the 2018 Met Gala (the "Gala Host Email"). McFARLAND told Employee-1 to show Victim-1 the Gala Host Email in person, which Employee-1 did. At the time, Employee-1 believed that the Gala Host Email was real. According to both Employee-1 and Victim-1, Victim-1 questioned the authenticity of the Gala Host Email.

14. Based on my discussions with employees of an American mass media company responsible for hosting the 2018 Met Gala, I have learned, in substance and in part, the following:

a. The Met Gala is an annual exclusive event thrown by a prominent fashion magazine (the "Magazine") for approximately 600 invited guests. The Met Gala is typically sold out by December. The vast majority of tickets are sold by invite only, and if a brand purchases a table, all guests must be approved by the Magazine. All guests must provide a biography and a photo. All tickets must be paid for and are non-transferrable. No third party ticket brokers were authorized to sell tickets to the Met Gala.

b. None of the victim customers who purchased tickets from NYC VIP Access were on the guest list for the 2018 Met Gala.

c. The Gala Host did not send the Gala Host Email, which purportedly confirmed the purchase of the victim's tickets.

15. Based on my discussions with Employee-1 and another law enforcement agent who interviewed Employee-1 and Employee-2, as well as reviewing that agent's notes and documents provided by Employee-1 and Employee-2, as well as my discussions with approximately 15 victims and review of their documents, I have learned that none of the victims received tickets for the 2018 Met Gala, and that WILLIAM McFARLAND, the defendant, caused the victims to be charged a total of over approximately \$36,000 for fraudulent 2018 Met Gala tickets.

The Burning Man 2018 Ticket Scam

16. Based on my discussions with Employee-1 and another law enforcement agent who interviewed Employee-1 and Employee-2, as well as reviewing that agent's notes and emails sent from the Employee-1 Email Account, I have learned, in substance and in part, that on or about January 4, 2018, WILLIAM McFARLAND, the defendant, sent email solicitations from the Employee-1 Email Account to a mass email list of prospective customers regarding ticket sales to Burning Man 2018, an annual counterculture event in Nevada's Black Rock desert from August 26 through September 3. The email with the subject "Burning Man 2018 - \$325 - 24 Hours" read as follows:

We were going to save this, but the snow in NYC today has us thinking of the playa. **We have 2018 Burning Man (8/26-9/3) passes today only for \$325 per person.** Ticket prices go up to \$525 tomorrow until we sell our allocation. Email me to reserve. PS - We will be able to help with camp invitations, parking passes, and more closer to Burning Man. (*emphasis in original*)

The email ends with the first name of Employee-1 and Employee-1's phone number.

a. According to Employee-1, McFARLAND told Employee-1 that sponsors for Burning Man 2018 provided tickets to

the event. Employee-1 sold one ticket to Burning Man 2018 at McFARLAND's direction.

b. According to Employee-2, customers made payments to the Employee-2 Payment Processor-2 Account for Burning Man 2018.

17. Based on my discussions with another law enforcement agent who interviewed employees of Burning Man 2018 and reviewing that agent's notes, I have learned, in substance and in part, the following:

a. Burning Man does not work with ticket resellers or entities, so third party ticket brokers cannot purchase tickets. Burning Man does not have any sponsors or partnerships. Groups or individuals must register for a profile on the Burning Man ticketing system in order to purchase tickets. Tickets went on presale on or about January 31, 2018, and then went on sale on or about March 28, 2018, and may be exchanged among registered ticket holders with profiles.

b. There was no record of any ticket purchases or transfers to either of the two victims who purchased Burning Man 2018 tickets from NYC VIP Access, or any ticket orders that contain the name of NYC VIP Access.

18. Based on my discussions with another law enforcement agent who interviewed Employee-1 and Employee-2 and my review of that agent's notes and documents provided by Employee-1 and Employee-2, as well as my discussions with a victim and review of the victim's documents, I have learned that neither of the two victims received tickets for Burning Man 2018, and that WILLIAM McFARLAND, the defendant, caused the victims to be charged a total of \$1300 for fraudulent Burning Man 2018 tickets. The victims made the payments to NYC VIP Access at the Employee-2 Payment Processor-2 Account.

The 2018 Grammy Awards Ticket Scam

19. Based on my discussions with a customer ("Victim-9") and review of Victim-9's documents, I learned that Victim-9 received an email purporting to be from a NYC VIP Access employee (the "Fake Employee") at an email account (the "Fake Employee Email Account") offering two tickets located in the 100-level for \$1,800. On or about November 25, 2017, Victim-9 made a payment of \$1,800 through an online payment system from New York,

New York. Victim-9 did not receive tickets to the 2018 Grammy Awards.

20. Based on my discussions with a customer ("Victim-5"), I have learned that Victim-5 and another customer ("Victim-6") each purchased tickets to the 2018 Grammy Awards for \$700 a ticket. Victim-5 flew from Florida to New York for the event, only for Victim-5 and Victim-6 to be rejected at the door.

21. Based on my discussions with another law enforcement agent who interviewed Victim-4 and Victim-8, and my review of that agent's notes and emails received by Victim-4, I have learned that another purported NYC VIP Access employee (the "Fake Employee") stated in an email from another NYC VIP Access email account (the "Fake Employee Email Account") that their tickets were located in the lower 100-level. However, the tickets for Victim-4 and Victim-8 were in a much higher level. As described below, Employee-2 believed that the Fake Employee was not a real person, and that McFARLAND used the Fake Employee Email Account.

**McFARLAND'S CONCEALMENT OF HIS OWNERSHIP AND CONTROL
OVER NYC VIP ACCESS**

22. Based on my discussions with another law enforcement agent who interviewed Employee-1 and Employee-2, and reviewing that agent's notes and documents provided by Employee-1 and Employee-2, I have learned, in substance and in part, the following:

a. According to Employee-1, WILLIAM McFARLAND, the defendant, stated that he wanted to hide his affiliation with NYC VIP Access because he feared that the bad press from the Fyre Festival and his criminal prosecution for alleged fraud related to the Fyre Festival would prevent NYC VIP Access from being successful. McFARLAND told Employee-1 that McFARLAND would operate NYC VIP Access from behind the scenes, and asked Employee-1 to be the face of the company, which Employee-1 agreed to do.

b. According to Employee-2, McFARLAND made Employee-1 the face of NYC VIP Access; Employee-2 believed this was because McFARLAND did not want people to know that NYC VIP Access belonged to him.

c. According to Employee-1 and Employee-2, McFARLAND took a number of steps to conceal his ownership and control of NYC VIP Access, as described more fully below.

23. WILLIAM McFARLAND, the defendant, sent Employee-1 a separation agreement (the "Separation Agreement") once he learned that Employee-1 became suspicious that NYC VIP Access was a scam. However, McFARLAND avoided including references to his identity as an owner of NYC VIP Access in that Separation Agreement. Specifically, based on my conversations with Employee-1 and another law enforcement agent who interviewed Employee-1, and my review of documents provided by Employee-1, I have learned the following:

a. In or about late March 2018, Employee-1 questioned McFARLAND about a customer's issues with Coachella tickets. When McFARLAND continued to come up with excuses, Employee-1 became concerned that NYC VIP Access was a sham. McFARLAND stated that Employee-1 should leave NYC VIP Access, which Employee-1 did.

b. On or about April 2, 2018, McFARLAND used an email address containing the name "billyzmcFarland" (the "McFarland Encrypted Email Account") to email a separation agreement (the "Separation Agreement") for Employee-1 to another employee who worked for McFARLAND ("Employee-3"). Employee-3 then forwarded McFARLAND's email to Employee-1. The Separation Agreement, which was never executed, purported to be between "BZM Projects and all of its Applicable Holdings, which includes but is not limited to its business and individual entities" and Employee-1, who is referred to as the "Contractor."¹ The Separation Agreement acknowledged that the "Contractor and Holdings are parties to numerous business dealings" and called for Employee-1 to agree to "a binding non-disclosure agreement for 5 years." The Separation Agreement also provided that the Holdings would immediately assume ownership of Employee-1's email accounts and messages therein as they pertained to the Holdings' business dealings.

c. Employee-1 did not sign the Separation Agreement because among other things, the Separation Agreement

¹ I know from my participation in this investigation that McFARLAND's initials are "BZM." I also learned from Employee-2 that McFARLAND used an email account with a "bzmprojects" domain name to email Employee-2 regarding NYC VIP Access business.

did not reference McFARLAND. McFARLAND had stated that BZM Projects was the holding company for McFARLAND's companies, including NYC VIP Access, but McFARLAND's name was nowhere in the Separation Agreement.

McFarland's Use of Employee-1 to Meet and Speak with Customers and Sign Paperwork on Behalf of NYC VIP Access

24. Based on my conversations with Employee-1 and another law enforcement agent who interviewed Employee-1 and Employee-2, and my review of that agent's notes and documents, I have learned, in substance and in part, the following:

a. At the direction of WILLIAM McFARLAND, the defendant, Employee-1 would meet with and call customers to solicit them to purchase tickets for events. McFARLAND did not meet or speak with customers.

b. McFARLAND directed that all contracts for ticket sales with customers be signed with Employee-1's name; however, McFARLAND created and finalized all contracts.

c. NYC VIP Access used electronic signatures to sign contracts. Based on my review of documents from an eSignature platform (the "eSignature Platform"), I have learned, in substance and in part, the following:

1. On or about September 5, 2017, an account was established in the name of Employee-3 with an email account that contains "billyzmcfarland" as the registered email address. To date, this account is active.

2. On or about December 21, 2017, an account was established in the name of Employee-1, with the username "NYC VIP Access." To date, this account is active. Based on my conversations with Employee-1, I know that Employee-1 has not paid for or used the eSignature platform since his departure from NYC VIP Access in late March 2018.

McFarland's Use of the Employee-1 Email Account

25. The investigation has revealed that while WILLIAM, McFARLAND, the defendant, wanted to provide the appearance that Employee-1 was responsible for communicating with victims through the Employee-1 Email Account, he in fact used the account to send communications to victims of the scheme. Specifically, based on my conversations with Employee-1 and another law enforcement

agent who interviewed Employee-1 and Employee-2, I have learned, in substance and in part, the following:

a. McFARLAND regularly corresponded with customers from the Employee-1 Email Account - an email account in Employee-1's name at NYC VIP Access. McFARLAND used the Employee-1 Email Account to send email solicitations about events to his mailing list, which included victims from the Fyre Festival. According to Employee-2, McFARLAND regularly read or showed the emails he was drafting to customers from the Employee-1 Email Account to Employee-1 and Employee-2 before he sent them.

b. McFARLAND did not have an email account in his own name at NYC VIP Access.

c. Employee-1 did not send any emails to customers.

d. According to Employee-2, at McFARLAND's direction, Employee-2 sent executed contracts to customers from the Employee-1 Email Account, but did not email with customers for any other purpose.

e. According to Employee-2, McFARLAND and his employees generally worked together at restaurants and work spaces. At no time did Employee-2 meet or communicate with the Fake Employee, whom McFARLAND would sometimes mention. McFARLAND used an email account that McFARLAND stated belonged to the Fake Employee Email Account, but then McFARLAND switched to using the Employee-1 Email Account.

26. IP logs² confirm that WILLIAM McFARLAND, the defendant, in fact had access to and used the Employee-1 Email Account and other accounts associated with Employee-1, across at least four different IP addresses. Specifically:

a. IP logs reflect common access to the Employee-1 Email Account from an e-mail address associated with McFARLAND. Specifically, based on my review of IP logs obtained from the eSignature platform, Google, and two customer-victims ("Victim-2" and "Victim-3"), I have observed the following logins from IP Address 207.97.151.192 ("IP Address-1") from December 15-21, 2017:

² IP addresses are a series of numbers that are used to uniquely identify a computer or computer network resource that is connected to the Internet.

1. On or about December 15 and 21, 2017, IP Address-1 was used to send an email from the Employee-1 Email Account to Victim-3.

2. On or about December 19, 2017, IP Address-1 was used to log into the Google account in the name of "Billy McFarland" and associated with an email including "billyzmcfarland" in the username (the "McFarland Google Email Account").

3. On or about December 21, 2017, IP Address-1 was used to log into the eSignature Platform account associated with the Employee-1 Email Account.

b. IP logs reflect access to the Employee-1 Email Account and the eSignature Platform account associated with the Employee-1 Email Account from an IP address associated with McFARLAND's parents. Specifically:

1. Based on my review of records from Verizon, I have learned that IP address 173.70.85.78 ("IP Address-2") was associated with an account belonging to "Steven McFarland" at an address in Morristown, New Jersey (the "New Jersey Address") from on or about July 11, 2017 through on or about February 16, 2018. I know from letters submitted to the court from the parents of McFARLAND that Steven McFarland is McFARLAND's father, and that he resides at the New Jersey Address.

2. Based on my review of IP logs from Payment Processor-1, the eSignature platform, and Victim-4, I have observed the following logins from IP Address-2 that resolves to the New Jersey Address of McFARLAND's parents, between December 25, 2017 through December 27, 2017: (1) on or about December 25, 2017, IP Address-2 was used to log into the Payment Processor-1 NYC VIP Access account associated with the Employee-1 Email Account; (2) on or about December 26, 2017, IP Address-2 was used to log into the eSignature Platform account associated with the Employee-1 Email Account; and (3) on or about December 27, 2017, IP Address-2 was used to send an email from the Employee-1 Email Account to Victim-4.

c. Similarly, IP logs reflect common accesses to McFARLAND's personal e-mail account (the McFarland Google Email Account), the Employee-1 Email Account, and other accounts

associated with Employee-1 from IP Address 206.71.252.236 ("IP Address-3") from December 28, 2017 through January 27, 2018:

1. On or about December 28 and 29, 2017, IP Address-3 was used to log into the Payment Processor-1 account associated with the Employee-1 Email Account.

2. On or about January 7 and 20, 2018, IP Address-3 was used to log into a software development account registered to the Employee-1 Email Account.

3. On or about January 15 and 27, 2018, IP Address-3 was used to log into the McFarland Google Email Account. Also, on or about January 15, 2018, IP Address-3 was used to log into the eSignature Platform account associated with the Employee-1 Email Account.

d. IP logs further reflect common accesses to McFARLAND's personal e-mail account (the McFarland Google Email Account), the Employee-1 Email Account, and other accounts associated with Employee-1 from IP Address 104.192.219.198 ("IP Address-4") from February 14, 2018 through February 15, 2018:

1. On or about February 14, 2018, IP Address-4 was used to log into the eSignature Platform account associated with the McFarland Email Account.

2. On or about February 15, 2018, IP Address-4 was used to send an email from the Employee-1 Email Account to Victim-2.

27. Based on my conversations with Employee-1 and another law enforcement agent who interviewed Employee-1 and Employee-2, as well as the above examples showing the same IP address logins from the personal accounts of WILLIAM McFARLAND, the defendant, and the Employee-1 Email Account and associated accounts, as well as certain of those logins occurring from an IP address that resolved to McFARLAND's parents' New Jersey residence, I believe that McFARLAND used the Employee-1 Email Account to contact NYC VIP Access customers in connection with the NYC VIP ACCESS ticket fraud scheme.

McFarland's Use of NYC VIP Access Employees' Accounts with
Payment Processors

28. Based on my conversations with Employee-1 and another law enforcement agent who interviewed Employee-1, and my

review of that agent's notes and other documents, I have learned, in substance and in part, that WILLIAM McFARLAND, the defendant, set up an account with Payment Processor-1 in Employee-1's name, and arranged for customer payments made by wire transfer or Payment Processor-1 to be deposited into Employee-1's bank account (the "Employee-1 Bank Account").

29. Based on my conversations with a Payment Processor-1 employee, as well as my review of documents from Payment Processor-1, I have learned, in substance and in part, the following:

a. The NYC VIP Access Account - which was registered in the name of Employee-1 - followed the same pattern as three prior accounts which were in the name of WILLIAM McFARLAND, the defendant, for Magnises, Fyre Festival and "William McFarland."³ For each of these accounts, there were large numbers of refunds sought based on customer complaints that purchased goods were not received. As a result, Payment Processor-1 discontinued the account, and noted that refunds that had been sought were unable to be provided to the vast majority of customers due to the substantial negative account balances associated with each account:

1. NYC VIP Access: -\$9,826.28.
2. Magnises: -\$62,543.02.
3. William McFarland: -\$519,030.00.
4. Fyre Festival: -\$767,641.76.

b. Payment Processor-1 also indicated that the same electronic device was used to access the NYC VIP Access account as the Magnises and Fyre accounts in McFARLAND's name.

30. Based on my training, experience and involvement in this investigation, as well as the common identifier and patterns among the NYC VIP Access Account and the Magnises and Fyre accounts, Employee-1's statement that McFARLAND opened the NYC VIP Access Account with Payment Processor-1 in Employee-1's

³ The following description of McFARLAND's business activity for his personal account was provided to Payment Processor-1: "Selling interactions with my followers and fans. I am the founder of Magnises. We work with you guys. This is a personal account for selling appearances, etc."

name and managed the account, the overlap in IP logins from the Payment Processor-1 account in Employee-1's name and McFARLAND's personal accounts, I believe that McFARLAND controlled the Payment Processor-1 account.

McFarland's Use of the Employee-1 Bank Account

31. Based on my conversations with Employee-1 and another law enforcement agent who interviewed Employee-1, I have learned, in substance and in part, that WILLIAM McFARLAND, the defendant, told Employee-1 that he did not have any bank accounts, and that it would take a few weeks to open a company bank account. McFARLAND asked Employee-1 to use the Employee-1 Bank Account for transacting NYC VIP Access business, as well as to pay for McFARLAND's lodging, food, transportation and utility bills as long as McFARLAND deposited sufficient funds to cover his expenses. Employee-1 agreed. McFARLAND proceeded to use Employee-1's bank account for several months, and continually provided excuses to Employee-1 as to why a bank account had not yet been opened in the company's name.

32. Based on my conversations with Employee-1 and another law enforcement agent who interviewed Employee-1, I have learned, in substance and in part, that Employee-1 identified the following NYC VIP Access business transactions, among others, made by WILLIAM McFARLAND, the defendant, in the Employee-1 Bank Account:

a. The following transfers of funds from "William McFarland" to the Employee-1 Bank Account: \$300 on December 4, 2017; \$500 on December 12, 2017.

b. Wire transfers of payments for tickets from three NYC VIP Access customers: i) Victim-5 in the amount of \$700 on November 30, 2017; ii) Victim-6 in the amount of \$700 on December 1, 2017; and iii) another victim ("Victim-7") in the amount of \$5,600 on December 22, 2017.

c. Numerous transfers of funds from Payment Processor-1 to Employee Bank Account-1, from in or about December 2017 up to and including in or about February 2018, totaling over \$138,000.

d. Based on conversations with Employee-1 and another law enforcement agent who interviewed Employee-1 and Employee-2, and approximately 15 victims, as well as my review of documents, I believe these funds described in above subparagraphs

b and c represent wire fraud proceeds from McFARLAND's fraudulent ticket scheme.

33. Based on my conversations with Employee-1 and another law enforcement agent who interviewed Employee-1, I have learned, in substance and in part, that WILLIAM McFARLAND, the defendant, made personal charges to the Employee Bank Account-1. For example, Employee-1 identified over approximately \$7,700 in charges from a hotel in New York, New York (the "Hotel") on multiple dates in January 2018. Based on my review of documents from the Hotel, I have learned that Employee-1 paid for a room at the Hotel using the Employee-1 Bank Account from December 27, 2017 to January 27, 2018. Throughout the duration of the stay at the Hotel, the names "William McFarland" and "Billy McFarland" were listed as an "Accompanying Guest."⁴

34. Based on my conversations with Employee-1 and another law enforcement agent who interviewed Employee-1, I have learned, in substance and in part, that Employee-1 identified the following charges that Employee-1 did not authorize, among others, made by WILLIAM McFARLAND, the defendant, from the Employee-1 Bank Account:

a. Charges from an Internet domain name registrar ("Domain Name Registrar-1") in January 2018 and March 2018.⁵ Specifically:

1. Based on my review of documents from Domain Name Registrar-1, I have learned that in or about January 2018, user account "Billy McFarland" used a payment card in the name of Employee-1 to reactivate the domain name "devmagnises.com," and register the domain names "bzmprojects.com" and "bzmbookings.com."

2. The same user "Billy McFarland" also registered the following domain names, among others: "fyreapp.com," "biajabookings.com," and "sousahouseny.com." I know from my participation in the investigation of McFARLAND that fyreapp.com is the Fyre Media website. I also know from online

⁴ From speaking with another law enforcement agent who interviewed Employee-2 and reviewing that agent's notes, I have learned, in substance and in part, that McFARLAND stayed at the Hotel.


⁵ Internet domain registrar allow individuals and companies to register names for websites.

source information that the "biajabookings" domain name is registered to "Billy McFarland," with an email account incorporating the name "billmcfarland." I also know from my participation in the investigation that the Sousa House is McFARLAND's current residence.

b. Outgoing wire transfers to a software development company (the "Software Development Company") of \$1,000 on January 9, 2018 and \$2,250 on January 18, 2018. Specifically, based on my review of documents from the Software Development Company, I have learned that an employee emailed "William McFarland" at an email address with the domain name "bzmprojects." The Software Development Company was assisting with the creation of a talent match making app known as "vybewithme". Based on my review of documents from Domain Name Registrar-1, I know that "vybewithme" is a domain name registered to the "Billy McFarland" user account.

35. Based on the numerous transactions conducted by WILLIAM McFARLAND, the defendant, in the Employee-1 Bank Account, I believe that McFARLAND had access to and control over the Employee-1 Bank Account. In addition, based on my training, experience and involvement in this investigation, I believe that McFARLAND caused wire fraud proceeds from the fraudulent ticket scheme to be transferred to the Employee-1 Bank Account for the purpose of concealing his ownership and control of the funds.

WHEREFORE, deponent prays that an arrest warrant be issued for the arrest of WILLIAM McFARLAND, the defendant, and that he be arrested and imprisoned or bailed, as the case may be.


BRANDON RACZ
SPECIAL AGENT
FEDERAL BUREAU OF INVESTIGATION

Sworn to before me this
11th day of June 2018


UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK